2015 年 7 月 22 日
NRI セキュアテクノロジーズ株式会社

サイバー攻撃に対応するガイドラインの販売を開始
～セキュリティインシデントへの対応力強化を支援～

NRI セキュアテクノロジーズ株式会社（本社：東京都千代田区、代表取締役社長：小田島 潤、以下「NRI セキュア」）は、サイバー攻撃をはじめとするセキュリティインシデント[*1] が発生した時に企業でとるべき対応手順や、事前準備から再発防止までの取るべき行動をまとめた冊子「インシデント対応ガイドライン」の販売を開始します。

本ガイドラインは、企業において設立から間もない CSIRT（シーサート：情報セキュリティインシデント対応体制）に配属された社員や、これまで独自のやり方でサイバー攻撃に対応してきた情報セキュリティ担当者に活用していただくためのものです。攻撃による被害を最小限にするためのコントロールに必要な知識の把握と、円滑な対応を行うための手順共有を可能にし、企業のインシデント対応力を強化することが狙いです。

■ 相次ぐサイバー攻撃への対応力の強化に有効

サイバー攻撃が日々発生する中、企業の CSIRT メンバーやセキュリティ担当者が対応しなければならない範囲はますます拡大しています。情報セキュリティに関する知識や対策は、常にメンバーや組織内で共有し、あらかじめ統一した見解や方針を定めておくことが望ましいものの、そのための議論の時間を確保し、関係者と合意を取り、従業員を教育していくことは容易ではありません。

ガイドラインを事前に準備しておくことで、インシデントや対応手順に関する知識の統一と共有ができれば、メンバー間での認識・知識レベルの差が少なくなり、対応の速度や質の向上に有効です。

■ インシデント対応時に役立つ現実的なマニュアル

セキュリティインシデントが発生した時の対応マニュアルを、CSIRT メンバーや情報セキュリティに知見のある人材が、公開されている資料をもとに作成することはできます。しかし、対応マニュアルができていることと、実際にインシデントが発生した際にマニュアルに沿って冷静に対応できることは異なります。

対応マニュアルでは、あらゆる角度から、起こりえる現実のインシデントに対応出来るノウハウが組み込まれていることが鍵となります。また、CSIRT がすべての脅威に対応できることは理想的ですが、そこに至るまでには多くの時間を要し、結果的に何も解決できない可能性があり、現実的とはいえません。そのため、実際に最も多いとされる外部から

の攻撃に絞って、現場に対応マニュアルを周知徹底することで、対応速度を上げることが求められます。

■ ガイドラインの主な内容

「インシデント対応ガイドライン」は、NRI セキュアが 2010 年から開始した「セキュリティ事故対策支援サービス[*2]」において、実際に現場で蓄積した対応ノウハウに加えて、NIST（アメリカ国立標準技術研究所）や SANS Institute[*3]、IPA（情報処理推進機構）など、複数の国内外の機関が発行する文献に沿って作成されています。

「対応が必要と想定される脅威（マルウェア[*4]感染、DDoS 攻撃[*5]など）」ごとに、事前準備から再発防止までの取るべき行動を 7 つのステップに分類し、インシデント対応における基本的な考え方や手順を解説しています。また、対応手順をより現場に浸透させることを目的として作成した、インシデント発生時に行うべき行動をまとめたハンドブックを付けています。

NRI セキュアは、今後も企業の情報セキュリティの強化や、サイバー攻撃への対策についての支援を行い、安全、安心な情報社会の実現に貢献していきます。

*1 セキュリティインシデント：ウイルスへの感染や不正アクセス、ウェブサイトの改ざんや情報漏えいなどのセキュリティに関する事故

*2 セキュリティ事故対策支援サービス：企業で発生した情報セキュリティ事故に対して、迅速かつ適切に対処するための、原因特定、影響範囲の調査、被害の拡散や再発防止、証拠保全といった事後対策を支援する NRI セキュアのサービス

*3 SANS Institute：政府や企業・団体における情報セキュリティに関連する研究、およびそれらに所属する人々の IT セキュリティ教育を目的として、1989 年に設立された組織（本部：米国ワシントン DC）。日本では NRI セキュアが事務局を運営

*4 マルウェア：コンピュータウイルスやワームなど、悪意のある不正なソフトウェアの総称

*5 DDos 攻撃：Distributed Denial of Service（分散サービス妨害）、複数の第三者のクライアントを踏み台にし、標的とするサーバに大量のパケットを同時送信し、サービス提供を不能にする攻撃

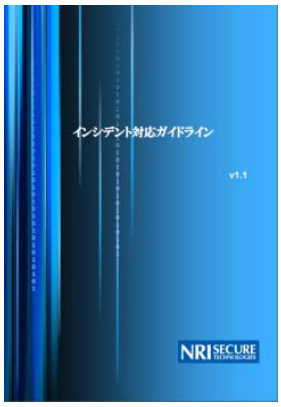
【ニュースリリースに関するお問い合わせ】
株式会社野村総合研究所　コーポレートコミュニケーション部　潘、十河
TEL：03-6270-8100　E-mail：kouhou@nri.co.jp
【本ガイドラインに関するお問い合わせ】
NRI セキュアテクノロジーズ株式会社　テクニカルコンサルティング部　藤原、小屋松
コーポレートコミュニケーション　根本
TEL：03-6706-0500　E-mail：info@nri-secure.co.jp

【ご参考】

■「インシデント対応ガイドライン」の価格および対象者

- 価格：100 万円＋税
- ガイドラインの利用想定対象者：
  企業における CSIRT や情報セキュリティおよび、インシデント対応の担当者。
  まだガイドラインが完備していない、CSIRT や情報セキュリティチーム。

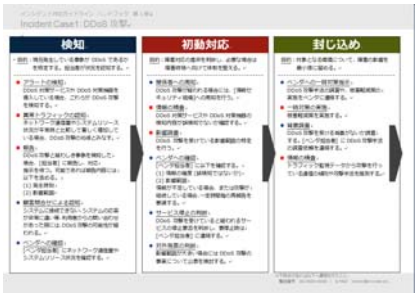
■ガイドライン本体の概要



- 体裁：A4 判　70 ページ（PDF にて提供）
- 扱っているインシデント項目：
- マルウェア感染
- DDoS 攻撃
- SQL インジェクション(情報漏えい)
- Web 改ざん
- フィッシング

■ハンドブックの概要

- 主な内容：インシデント発生時に対応すべき点を、ガイドラインより要約
- 体裁：A4 判　10 ページ（PDF にて提供）



■インシデント対応の 7 つのステップ（ガイドラインより）